DTIRP Arms Control Security Information Article
A PRODUCT OF THE DEFENSE TREATY INSPECTION READINESS PROGRAM, DECEMBER 2004
Order Number 947A

Arms Control Security Vulnerability Assessment Process

Many sites and facilities are potentially vulnerable to arms control verification activities, including on-site inspections. To assist facilities in protecting sensitive information during such inspections, the Department of Defense (DoD) sponsors vulnerability assessments under the Defense Treaty Inspection Readiness Program (DTIRP). Upon request, DTIRP assessment teams are available to visit these facilities, conduct site-specific assessment analyses, and recommend cost-effective countermeasures to protect national security, proprietary, and other sensitive information. This article outlines the purpose, personnel, and processes DTIRP uses to conduct arms control security vulnerability assessments.

Background

As a result of international arms control treaties and agreements, an increasing number of facilities are subject to on-site inspections. These inspections serve to help verify and demonstrate U.S. treaty compliance. These on-site inspections are conducted by foreign inspection teams and are potentially intrusive. However, the United States retains the right to protect from improper disclosure national security, proprietary, or other sensitive information not essential to verification objectives. With this in mind, DTIRP, in conjunction with other DoD organizations, developed the arms control security vulnerability assessment process as a means to assist facility personnel in identifying and protecting sensitive information during arms control verification activities.

Assessment Purpose

The arms control security vulnerability assessment process evaluates a facility or site to determine its potential vulnerability to arms control verification activities and develops cost-effective security countermeasures to protect at-risk sensitive information. The ultimate aim of these efforts is to assist facilities in protecting sensitive information from inadvertent or unnecessary disclosure during arms control verification activities.

Assessment Team Composition

Vulnerability assessment teams employ arms control experts with specialized backgrounds to provide advice and assistance to facilities. Assessment teams may include a wide range of security specialists from Service Components and independent agencies, as well as personnel with experience in arms control verification activities from various organizations within the arms control community.

A typical team may include specialists in technology transfer, industrial security, information security, operations security, counterintelligence, arms control agreements, and treaty escorting procedures. Specific team composition is tailored to the needs of the particular facility being assessed.

Team members are typically drawn from the following organizations:

- Defense Intelligence Agency
- Defense Security Service (DSS)
- Defense Threat Reduction Agency (DTRA)
  - Arms Control Interagency Liaison Division
  - Counterintelligence Office

  - On-Site Inspection Directorate, Operations Support Division, Countermeasures Branch
- DoD
  - Nuclear Treaty Programs Office
  - Treaty Management Office
- Department of Energy
- Department of the Air Force
  - Office of Special Investigations
- Department of the Army
- Department of the Navy
  - Naval Criminal Investigative Service
- Federal Bureau of Investigation
- Interagency OPSEC Support Staff
- Joint Staff
- National Security Agency

Assessment Methodology

Vulnerability assessments are conducted using a five-phase approach. While each phase is distinct, phases I and II may run concurrently.

Phase I: Coordination

The first phase of an assessment begins with an assessment request.[1] Receipt of a customer request triggers a number of activities required to properly plan and prepare for the assessment. The focus is on gathering and consolidating facility or program information, identifying applicable arms control treaties or agreements, defining personnel and logistical requirements, and developing an assessment mission plan.

To facilitate these efforts, a single point of contact (POC) is established in the On-Site Inspection Directorate's Operations Support Division, Countermeasures Branch of DTRA during this phase. The POC's role is to facilitate communication and coordination with the requesting facility or program and its parent organization. Most coordination entails arranging the participation of the various team members and finalizing logistical arrangements for the visits.

[1]DTIRP's support services, including vulnerability assessments, are coordinated and approved by the cognizant head of the DoD component. Each Military Service has a program office responsible for coordinating these types of support requests, and they work closely with DTIRP.

The assessment team POC first contacts the requesting facility to conduct an initial interview. During the interview, the POC describes the assessment process, solicits facility background data, and ascertains whether there has been any self-assessment or previous outside assessment conducted. If such an assessment has previously been conducted, the POC will request copies of the report(s).

Phase II: Open Source Data Search and Assessment Team Training

While foreign inspection teams base their inspection plans primarily on information contained in required data declarations, they usually supplement the declarations with information gathered through open sources. With the explosive growth of the Internet, an unprecedented amount of information is available.

For this reason, a DTIRP member on the assessment team conducts a Web-based data search to gain an understanding of the type of open source information available about the facility in question. The data is compiled in a Facility Profile Report, which addresses such areas as operations, defense programs, personnel, financial status, and geographic data. This report enables team members to predict possible inspection scenarios and to conduct preliminary analyses of viable, treaty-compliant, security countermeasures. The report also helps assessment team members in preparing for and focusing the assessment tasks.

After the Facility Profile Report is complete, the entire team gathers for pre-deployment training. This training includes a review of specific provisions of the applicable arms control treaty or agreement, and their applicability to the facility being assessed.

Phase III: Pre-Assessments

An on-site pre-assessment is often conducted to validate and focus the requirement for a full-scale assessment. During the pre-assessment, the team identifies assets, programs, and essential elements of sensitive information potentially at risk due to their nature or proximity to an inspectable area or program. Teams may also conduct a pre-assessment in anticipation of treaty ratification, entry into force, or an initial treaty-required declaration submission.

During the pre-assessment phase, the assessment team may determine that further assessment visits are unnecessary. If further visits are needed, assessment team personnel will begin to integrate site personnel into the assessment team, and determine the scope and personnel requirements for a full-scale assessment.

Phase IV: Assessments

Full-scale assessments are conducted to address the treaty, technology transfer, industrial security, physical security, counterintelligence, and information security issues identified during the pre-assessment. The assessment team seeks to develop treaty and/or location-specific, cost-effective security countermeasure recommendations to protect sensitive information in advance of arms control verification activities. Each assessment team is specifically tailored to provide the expertise necessary to accomplish the assessment tasks for each location. A typical team can consist of eight or more members depending on the size of the facility, the technologies involved, and the areas to be assessed.

After an introductory briefing by facility staff, the assessment team chief introduces the team members and presents an overview briefing of the assessment process. The team chief then outlines the assessment tasks, activity timeline, final products and expected outcome. The assessment process itself consists primarily of data collection—accomplished through briefings, interviews, tours and record reviews. Standardized assessment worksheets are used throughout the process to record this data. The information acquired is collated and analyzed to form a picture of facility operations, personnel, and programs. The more accurate and complete this picture is, the better able the assessment team will be to assess the vulnerability of sensitive information.

To maximize the effectiveness of the assessment, it is important for the facility to identify sensitive information protection practices, any unique on-site security or operational procedures, and any other pertinent information that may be helpful to the assessment team. During the assessment process, the team will usually operate in a number of subgroups for efficiency and then meet together as a group each evening to collate and crosscheck information, and to plan subsequent assessment tasks.

Phase V: Reporting

Upon conclusion of an assessment, facility representatives may be given a 1-2 page “Quicklook” assessment report that recounts the team's observations and summarizes any major issues. The Quicklook report can either help to confirm the effectiveness of using existing security measures in an arms control inspection environment; or, if inadequacies are detected, serve as a guide for effective inspection preparation, and if necessary, the application of appropriate countermeasures.

The Quicklook report is augmented later with information gleaned from team members' assessment worksheets, collected facility documentation, and other information necessary to complete the draft assessment report. The draft assessment report includes a program-by-program, building-by-building assessment of potential vulnerabilities and recommendations for appropriate security countermeasures. The completed draft assessment report is then forwarded to the requesting agency or Service for review and approval. At a minimum, draft assessment reports will be handled as For Official Use Only (FOUO). The final assessment report will incorporate the comments of the requesting agency or Service.

Conclusion

The arms control security vulnerability assessment process is a valuable tool for assisting a Military Service or DoD agency in evaluating the preparation needs of a given facility for either single or multiple treaty regimes. All of the Military Services have centralized arms control compliance and implementation program offices that coordinate and approve Service facility requests for DTIRP support. In some cases, Service counterintelligence and security organizations already provide these types of assessments.

To obtain additional information about the arms control security vulnerability assessment process and the application of security countermeasures, contact the DTIRP Outreach Program coordinator at 1-800-419-2899 or dtirpoutreach@dtra.mil, your local DSS Industrial Security Representative, or your government sponsor.